REMARKS

Claims 1-13 are pending in the instant application (hereinafter, the "'320 Application").

Response to the Notice of Non-Compliant Amendment

In the Notice of Non-Compliant Amendment, the Examiner asserts that each claim has not been provided with a proper status identifier, and as such, the individual status of each claim cannot be identified. We respectfully disagree. A copy of the claim set filed 26 September 2007, as downloaded from the Patent Application Information Retrieval system ("PAIR") is attached hereto as Appendix A. Each and every one of claims 1-13 was indeed provided with an acceptable status identifier, per MPEP §714(c).

Claim 7 is amended to resolve the Examiner's objections. We have compared the claims filed 26 September with the originally-filed claims, and have found no other un-marked amendments. No new matter is added with the amendments presented herein.

It is believed that the above amendments and the remarks filed 26 September 2007 are fully responsive to both the Notice of Non-Compliant Amendment and the Office Action of 26 March 2007. Per instructions on the Notice of Non-Compliant Amendment, Applicants submit only the corrected Amendments to the Claims, herewith. Please refer to the Remarks filed with the Response to the Office Action dated 26 September 2007 for arguments regarding the rejections and objections presented in the Office Action dated 26 March 2007.

Request for Correction of Material Mistake Made by the Office in the Applicant's Record (on PAIR)

U.S. Patent Application Serial No. 10/758,852 claims priority to the '320 Application. See Appendix B, Related Applications, paragraph [0002]. However, PAIR does not include U.S. Patent Application Serial No. 10/758,852 as a child application of the '320 Application in the Continuity Child Data. Correction of the Child Continuity Data for the '320 Application in PAIR, to include U.S. Patent Application Serial No. 10/758, 852, is respectfully requested.

CONCLUSION

We believe that the attached corrected Amendments to the Claims and the remarks laid out above address and resolve each objection presented in the Notice of Non-Compliant Amendment mailed 11 December 2007. We respectfully request the Examiner's consideration of the amendments presented herein, and the Remarks filed 26 November 2007.

This paper is timely filed within one month of the mailing date of the Notice of Non-Compliant Amendment. No fees are believed due; however, if any fee is deemed necessary in connection with this paper, please charge Deposit Account No. 12-0600. Should any issues remain outstanding, the Examiner is encouraged to telephone Applicants' attorney, Curtis A. Vock, at (720) 931-3011.

Respectfully submitted,
LATHROP & GAGE L.C.

Date: 1/11/08

By: _____

Mimi Nguyen, Reg. No. 59,150
4845 Pearl East Circle, Suite 300
Boulder, Colorado 80301
Telephone: (720) 931-3038
Facsimile: (720) 931-3001

Appendix A

Atty. Docket No. 413130

IN THE CLAIMS

Please amend the claims as follows:

1. (Original) A method of non-centralized zero-knowledge authentication for a computer network, comprising steps of:

establishing a first computer having a first authentication agent and a first prover agent on the computer network;

detecting a first authentication request over the computer network from a second computer having a second prover agent;

authenticating the second prover agent through a zero-knowledge identification protocol; and

promoting the second computer with a second authentication agent to perform authentication for the computer network.

2. (Currently Amended) The method of claim 1, further comprising periodically generating and distributing a new secret to the first and second authentication agents.

3. (Original) The method of claim 1, further comprising:

detecting a second authentication request over the computer network from a third computer having a third prover agent;

authenticating the third prover agent through a zero-knowledge identification protocol with the second authentication agent; and

promoting the third computer with a third authentication agent to perform authentication for the computer network.

4. (Currently Amended) The method of claim 1, further comprising periodically publishing encrypted numbers for the zero-knowledge identification protocol, including the steps of:

generating [[a]] first and second large prime numbers;

calculating a product of the first and second large prime numbers;

Atty. Docket No. 413130

generating a secret to have a value relatively prime to the product, greater than zero and less than the product;

encrypting the product;

encrypting the secret; and

publishing encrypted values of the secret and product.

5. (Currently Amended) A method of protecting a host from unauthorized client access over a network, comprising the steps of:

~~creating~~installing a prover agent application on the client;

~~creating~~installing a verifier agent application on the host;

creating a trusted source application to generate and publish encrypted values of a secret and product of first and second large prime numbers;

reading the encrypted values for the secret and product, by the prover and verifier from the trusted source;

decrypting the secret, by the prover and verifier;

decrypting the product, by the prover and verifier; and

performing a plurality of verification dialog between the prover and verifier, wherein the prover demonstrates knowledge of the secret and product without exposing the values of the secret and product, and wherein the client is denied access to a secure area of the host when the prover fails to demonstrate knowledge of the secret and product and granted access to the secure area when the client succeeds in demonstrating knowledge of the secret and product.

6. (Original) The method of claim 5, wherein the steps of decrypting the secret and product further utilize previous values of the secret and product as operators in the modulus inverse operations.

7. (Currently Amended) The method of claim 5, further comprising:

~~creating~~installing a first agent to be authenticated, the first agent having values for s, n and t, s being the secret, n being the product, and t being a size of an answer set;

Atty. Docket No. 413130

~~creating~~installing a second agent to authenticate the first agent, the second agent having values for s, n, and t;

generating r as a random number generated by the first agent;

calculating x by the first agent, r being raised to power of t modulus n;

sending x from the first agent to the second agent;

calculating b by the second agent, b being further defined as a member of set of integers from zero through t-1;

sending b from the second agent to the first agent;

calculating y by the first agent, y being a product of r*s raised to power of b;

sending y from the first agent to the second agent; and

determining authentication of the first agent, by determining equivalence of a first equation to a second equation, if y is not equal to zero, first equation is y{circumflex over ( )}t mod n and second equation is (xv{circumflex over ( )}b) mod n.

8. (Original) A system of non-centralized zero-knowledge authentication for a computer network, comprising:

two or more computers establishing the computer network, each of the computers containing an authentication agent, secret and prover agent; and

a requesting computer having a prover agent, for requesting access to the computer network,

wherein the prover agent of the requesting computer and one of the authentication agents of the two or more computers engaging in a zero-knowledge authentication protocol, and wherein the requesting computer operates with an authentication agent on the computer network when the requesting computer is authenticated through the zero-knowledge authentication protocol.

9. (Original) The system of claim 8, further comprising a trusted source for periodically generating a new secret for the authentication agents of computers on the network.

Atty. Docket No. 413130

10. (Original) The system of claim 8, the requesting computer comprising a cell phone.

11. (Currently Amended) The system of claim 8, the computer network comprising one or more of the Internet, ~~LAN~~a local area network, a communications link, and a wireless network.

12. (Original) The system of claim 8, the authentication agents and prover agents being installed on each of the computers through common software.

13. (Original) A software product comprising instructions, stored on computer-readable media, wherein the instructions, when executed by a computer, perform steps for non-centralized zero-knowledge authentication for a computer network, comprising:

instructions for establishing a first computer having a first authentication agent and a first prover agent on the computer network;

instructions for detecting a first authentication request over the computer network from a second computer having a second prover agent;

instructions for authenticating the second prover agent through a zero-knowledge identification protocol; and

instructions for promoting the second computer with a second authentication agent to perform authentication for the computer network.

Appendix B

PATENT
Attorney Docket No: 413127
Express Mail Label No. EV 386864945 US

SYSTEMS AND METHODS FOR ENTERPRISE SECURITY WITH COLLABORATIVE PEER TO PEER ARCHITECTURE

RELATED APPLICATIONS

[0001] This application claims priority to: U.S. provisional patent application no. 60/440,522 titled "Exploits in Database Methods and Systems," filed on 16 January 2003; U.S. provisional patent application no. 60/440,656, titled "Pattern Recognition Systems and Methods," filed on 16 January 2003; and U.S. provisional patent application no. 60/440,503, titled "Collaborative Peer-To-Peer Architecture," filed on 16 January 2003, incorporated herein by reference.

[0002] This application also claims priority to U.S. Non-provisional Patent Application No: 10/687,320, titled "System and Method of Non-Centralized Zero Knowledge Authentication for a Computer Network," filed on 16 October 2003.

BACKGROUND

[0003] A computer system may contain many components (e.g., individual computers) that are interconnected by an internal network. The computer system may be subject to attack from internal and external sources. For example, the computer system may be attacked when portable media (e.g., a USB drive) is used in by one or more components of the computer system. In another example, the computer system may be attacked when a connection is made (by one or more components) to an external communication device, such as when an individual computer connected to the computer system uses a modem to connect to an information service provider (ISP). In another example, the computer system may be attacked through a permanent connection to the Internet. In another example, the computer system may be attacked through a permanent connection to an internal network (LAN) connected to the Internet. Such attacks may be intended to cripple the targeted computer system either temporarily or permanently, or may instead settle to acquire confidential information, or both. One type of attack may be